CLAIMS

1. A method of encrypting identification tags of the type having a data storage for storing a fixed tag UID unique to each of said tags and variable user data, said tag UID and said user data being readable by a tag reader, said method comprising the steps of:

providing an identification tag having a permanent UID stored thereon;

providing an encryption engine operative for encrypting user data with an encryption key;

entering said UID to provide part or all of said encryption key;

entering user data for encryption by said engine;

encrypting said user data with said encryption key to derive encrypted user data; and

storing said encrypted user data in said data storage of said identification tag.

2. The method of Claim 1 wherein said tag is an RFID tag and said data storage is readable by an RFID reader.

3. The method of Claim 1 wherein said encryption engine comprises an encryption algorithm running on a digital processor platform enabled for reading and writing to said data storage.

4. The method of Claim 3 wherein said digital processor platform is operatively associated with an RFID reader for reading and writing to said data storage.

5. The method of Claim 3 wherein said encryption algorithm is a DES encryption algorithm.

6. The method of Claim 1 wherein said encryption key is a final key based on a combination of said tag UID and a private key.

7. The method of Claim 6 wherein said final key is derived by XORing said private key with said tag UID.

8. A method of decrypting encrypted user data stored on an encrypted identification tag, comprising the steps of:

providing a decryption engine operative for decrypting said encrypted user data with an encryption key;

presenting an encrypted identification tag for reading;

reading said tag UID and said encrypted user data stored on said encrypted identification tag;

providing said tag UID to said decryption engine for deriving said encryption key;

providing said encrypted user data to said decryption engine for decryption with said encryption key; and

decrypting said encrypted user data with said decryption engine to derive decrypted user data.

9. The method of Claim 8 wherein said encrypted identification tag is an RFID tag and said tag is readable by an RFID reader.

10. The method of Claim 8 wherein said decryption engine comprises a decryption algorithm running on a digital processor platform enabled for reading and writing to said encrypted identification tag.

11. The method of Claim 10 wherein said digital processor platform is operatively associated with an RFID reader for reading and writing to said encrypted identification tag.

12. The method of Claim 10 wherein said decryption algorithm is a DES decryption algorithm.

13. The method of Claim 8 wherein said encryption key is a final key based on a combination of said tag UID and a private key.

14. The method of Claim 13 wherein said final key is derived by XORing said private key with said tag UID.

15. A method for encrypting and decrypting user data stored on identification tags of the type having a UID code on each tag, comprising the steps of generating a key based in part or in whole on said UID code of one said tag, encrypting said user data with said key to derive encrypted user data for storage on said one tag, and decrypting encrypted user data read from said one tag with said key, such that a unique key is generated for encryption and decryption of user data on each tag.

16. The method of Claim 15 wherein said identification tags are RFID tags.